

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION CONTAINED IN
CELLULAR TELEPHONES:

APPLE IPHONE, THREE REAR
CAMERAS, TAN WITH BROWN CASE
("Device 1");

APPLE IPHONE, RED WITH GRAY
TRANSPARENT CASE ("Device 2").

Case No. 2:21-cr-758

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR
A WARRANT TO SEARCH AND SEIZE**

I, Keith Herriott, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer (TFO) with the United States Federal Bureau of Investigation (FBI), and have been assigned to the FBI since March of 2019. I have been a sworn law enforcement officer for the Charleston County Sheriff's Office (CCSO) since March of 2007. I was first assigned to the patrol division and patrolled the streets of Charleston County in uniform and a marked police car. In February of 2009, I was assigned to Forensic Services Unit of CCSO. My duties and responsibilities focused on the processing of crime scenes and preservation of

evidence to be processed for crimes. In August of 2011, I was assigned to the Criminal Investigation Division of the CCSO. My duties and responsibilities focused on the investigation of violent crimes, financial crimes and special victims in the jurisdiction of the county of Charleston. Since March of 2019, I was assigned to the Charleston FBI Task Force and my duties and responsibilities shifted to investigating violent gangs operating inside and outside the borders of the United States. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7), and empowered by federal law to investigate and make arrests for offenses enumerated in Section 2518 of Title 18 of the United States Code. As a Task Force Officer, I have been trained in various aspects of law enforcement, particularly in general investigation techniques. During my experience with CCSO and FBI, I have participated in hundreds of investigations and prosecutions. In connection with those investigations, I have conducted surveillance, executed searches, and secured relevant information using numerous other investigative techniques.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is: (1) an Apple iPhone, three rear cameras, tan with a brown case (**Device 1**) and (2) an Apple iPhone, red with a gray transparent case (**Device 2**) (collectively, "**the Devices**"). **Devices 1 and 2** are currently located in a Charleston Police Department Evidence Room.

5. The applied-for warrant would authorize the forensic examination of **the Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On September 8, 2021, TFO Jerome De Sheers was contacted by Tulsa Police Department (TPD) Detective Robbie Bowman in reference to subjects involved with a theft of a motor vehicle, which was used to complete a theft from an Automated Teller Machine (ATM), in Tulsa, Oklahoma. TPD Detective Bowman also advised that a silver 2016 Chevrolet Impala, with Texas temporary license plate bearing the digits "20049F9" (VIN 2G11X5SA6G9122454) which was used by the suspects in connection with both crimes, was in Charleston, South Carolina, and was frequenting the area of 2237 Savannah Highway (Quality Inn).

7. TPD Detective Bowman advised that he also had information that Andre Omar MARTIN was one of the subjects that was in Charleston, South Carolina with the vehicle, after video surveillance captured Andre Omar MARTIN at Walmart, located at 3951 West Ashley Circle, Charleston, South Carolina, on the morning of September 8, 2021.

8. FBI Special Agents and TFO's conducted a physical surveillance at 2237 Savannah Highway (Quality Inn) and observed the Chevrolet Impala parked in the parking lot. Multiple subjects were observed going from the vehicle to Room 247, which included individuals later confirmed to be Torrence Ramon WHITAKER and Andre Omar MARTIN.

9. Law enforcement continued surveillance on the Chevrolet Impala, which travelled through several Charleston area neighborhoods and apartment complexes.

10. In the early morning hours of September 9, 2021, law enforcement officers surveilled the Chevrolet Impala to Wildts Battery Boulevard, Johns Island, South Carolina, where an individual exited the Chevrolet Impala and proceeded to steal a white 2004 Ford F-250, with South Carolina license plate bearing the digits "RWP822" (VIN 1FTNW21P94ED55592). The

vehicle was taken from Wildts Battery Boulevard but was then parked a short distance away on Towne Street.

11. The Chevrolet Impala was then surveilled back to the Quality Inn where the occupants returned to Room 247. After approximately one hour, the occupants, including Torrence Ramon WHITAKER and Andre Omar MARTIN exited Room 247 carrying items to the trunk of the Chevrolet Impala before going back to the location where the Ford F-250 was parked.

12. After the Chevrolet Impala returned to the Ford F-250, the co-conspirators then began to hook chains to the rear of the Ford F-250 and a short time later both vehicles left the location where the Ford F-250 was parked. The F-250 left the area and went directly to the Chase ATM located at 2770 Maybank Highway, Charleston, South Carolina. The Ford F-250 backed up to the ATM when three individuals used crow bars, chain, and hooks to remove the housing of the ATM, exposing the safe.

13. Law enforcement arrived at the Chase ATM and attempted to take all co-conspirators into custody, however three subjects fled on foot. A fourth subject from the Ford F-250, Andre Omar MARTIN, was apprehended from inside the bed of the pickup truck after fighting with the law enforcement. Andre Omar MARTIN was in possession of **Device 1**. When officers recovered **Device 1** it was displaying a map with the direction of travel from Houston, Texas to Charleston, South Carolina on its home screen.

14. A traffic stop was conducted on the Chevrolet Impala after it left the Ford F-250 and drove past the Chase ATM while officers were attempting to apprehend the occupants of the Ford F-250. The driver and sole occupant of the Chevrolet Impala at that time was Torrence Ramon WHITAKER. Connected to a power cable and sitting on the driver's seat was **Device 2**. I know, based on training and experience, that **Device 2** has the capabilities of tracking location and map

features that would be used by Torrence Ramon WHITAKER to assist with driving around in unfamiliar locations, due to Torrence Ramon WHITAKER not being from the Charleston, South Carolina area.

15. Chase Bank security reported to the Charleston Police Department Detective Kevin Mapp that \$15,880 in U.S. Currency was contained in the ATM.

16. **The Devices** are currently being in the Charleston City Police Department Evidence Room. In my training and experience, I know that **the Devices** have been stored in such a manner that their contents remain, to the extent material to this investigation, in substantially the same state as they were when **the Devices** first came into the possession of the FBI.

17. Based on my training, experience, and discussions with other investigators with experience in the subject matter, there is probable cause to believe that **the Devices** will contain evidence of violations of Title 18 U.S.C. §§ 2113(b) and 371.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer

a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of

electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving

them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- h. Cloud Services: The device may utilize storage locations in addition to that of the physical memory chip within the device which may be removable or may be contained in “cloud” storage locations. The device accesses these locations or devices via settings, options, and programming contained within the device itself, which results in the direct deposit or retrieval of data from these locations. Additionally, the common method of data backup for the device is through a cloud-

based service which stores previous copies of the selected backup data for the accounts associated with the device.

19. Based on my training, experience, and research I know that each Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, a PDA, and access to cloud based sources. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of **the Devices** described in Attachment A to seek the items described in Attachment B.

This affidavit has been reviewed by Assistant United States Attorney Nick Bianchi.

Respectfully submitted,



Keith Herriott
Task Force Officer
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 13th day of September, 2021, at approximately 2:53 p.m.



MOLLY H. CHERRY
UNITED STATES MAGISTRATE JUDGE

